



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/779,440	02/09/2001	Kentaro Shiomi	60188-031	6677

7590 06/14/2006  
MCDERMOTT WILL & EMERY  
600 13TH STREET, N.W.  
WASHINGTON, DC 20005-3096

EXAMINER

KIM, JUNG W

ART UNIT PAPER NUMBER

2132

DATE MAILED: 06/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No.	Applicant(s)	
	09/779,440	SHIOMI ET AL.	
	Examiner	Art Unit	
	Jung Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 28 April 2006.  
2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.  
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-7, 24 and 25 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
5) ☒ Claim(s) 2-7 is/are allowed.  
6) ☒ Claim(s) 1, 24 and 25 is/are rejected.  
7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.  
8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.  
10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☒ All b) ☐ Some \* c) ☐ None of:  
1. ☒ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).  
\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

1. This Office action is in response to the amendment filed on 4/28/06.
2. Claims 1-7, 24 and 25 are pending.
3. Claims 8-23 are canceled.
4. Claims 1, 24 and 25 are amended.

### ***Response to Arguments***

5. The 112, 2<sup>nd</sup> paragraph rejections to claims 1, 24 and 25 as omitting essential structural cooperative relationships of elements and essential elements are withdrawn in view of applicant's arguments. In particular, applicant's arguments that "[t]he particular mechanism by which conversion of the circuit design data into encrypted design data is effected and the value of the key data are not essential for operation of the invention in its entire, broad scope ... [t]he claims need not recite the particular manner by which the key data corresponds to the encrypted circuit design data to effect the "unlocking" thereof..." are persuasive.

6. Applicant's arguments on pgs. 9-10, with respect to the prior art rejections of claims 1, 24 and 25 have been fully considered but are not persuasive. Specifically, Applicant's argue that the prior art does not teach the step of "the circuit design data is selected to operate as targeted when the (real) key data is inputted into the LSI after the step of converting the circuit design data into encrypted circuit design data." Examiner disagrees with applicant's contention. On section 4.2 "Insert Dead or Irrelevant Code",

Collberg discloses using a predicate to select between two obfuscated code segments at runtime; these code segments are generated using different obfuscation techniques on the original code segment. As articulated in the "Response to Arguments" section of the previous Office action, mailed on 11/28/05, the predicate operates as a selection signal and is consistent within the meaning of a key value as disclosed in applicant's Specification and claims. This interpretation of the new limitation in view of the prior art is consistent with applicant's own admission of the essential nature of the claimed invention. (*supra*) Therefore, since the selection of the predicate is determined at runtime and the selection at runtime enables the encrypted circuit design to run as targeted, the prior art of record discloses the new limitation.

7. In reply to applicant's argument that Collberg teaches away from accessing the alleged dummy data (pg. 10, 1<sup>st</sup> full paragraph), examiner disagrees and directs applicant's attention to fig. 4(b), wherein at runtime, either of one of two paths are selected.

8. Finally, in reply to applicant's argument that Collberg is completely silent as to the alleged dummy design data having the same number of inputs/outputs as the real circuit, examiner respectfully disagrees for two reasons. First, circuit design principles conventionally require groups of bits, which are fixed in size, to be transferred between circuit modules (16, 32 or 64 bit words are standards). Dummy circuits combined with "real" circuits would obey the standards of the circuit design and incorporate fixed data inputs and outputs corresponding to the number of bits comprising a word to be transferred to maintain the stealth of the obfuscation transformation (Collberg, section

3.2.2; a dummy circuit having a number of data inputs and/or outputs different from the conventional word size is conspicuously distinct from the other circuits). Second, the branch instruction between two flow paths as identified in figure 4(b) of Collberg shows two parallel code segments ( $S^a$  and  $S^b$ ) wherein both obfuscated code segments take in equivalent inputs and outputs identical values. Moreover, since Johnson discloses that hardware design and high-level programming languages are generally encoded based on similar principles (Johnson, col. 7:67-8:48), this disclosure of Collberg suggests having the same number of inputs/outputs as the real circuit. Hence, the amended claims remain rejected as being unpatentable over the prior art of record.

### ***Claim Rejections - 35 USC § 112***

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 1, 24 and 25 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

11. Claims 1, 24 and 25 define the limitation "wherein the circuit design data is selected to operate as targeted when the key data is inputted into the LSI after the step of converting the circuit design data into encrypted circuit design data." However, the limitation is indefinite because the language of the claim suggests selecting to operate the circuit design data using the generated key data when the key data is inputted into the LSI **after the step of converting** the circuit design data into encrypted circuit

design data. On the face of the limitation, this is not feasible because the circuit design data is converted into encrypted circuit design data at the time of selection.

***Claim Rejections - 35 USC § 103***

12. Claims 1, 24 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Johnson et al. USPN 6,088,452 (hereinafter Johnson) in view of Collberg et al. "Manufacturing Cheap, Resilient, and Stealthy Opaque Constructs" (hereinafter Collberg).

13. As per claim 1, Johnson discloses a method for designing a circuit, comprising the step of encrypting provided circuit design data (Johnson, Abstract), the encrypting step includes the steps of:

- a. generating dummy circuit design data; converting the circuit design data into encrypted circuit design data by combining the circuit design data and the dummy circuit design data (Johnson, col. 12:9-20).

14. Johnson does not expressly disclose generating key data, wherein the circuit design data is selected to operate as targeted when the key data is inputted into the LSI after the step of converting the circuit design data into encrypted circuit design data. Collberg discloses multiple opaque constructs wherein irrelevant code is inserted into an original code by means of a branch insertion transformation (Collberg, fig. 4(b)); a basic block is replaced with two different obfuscated versions by applying different sets of obfuscating transformations to the basic block. At runtime, a predicate selects one of

Art Unit: 2132

two paths, the operation of the code being equivalent regardless of the selection of the paths. (Collberg, section 4.2, 3<sup>rd</sup> paragraph) This runtime value is the key data of the obfuscation technique disclosed by Collberg. Moreover, although Collberg discloses such limitations in the context of software design rather than hardware design, the two areas are closely linked: Johnson discloses that hardware design and high-level programming languages are generally encoded based on similar principles (Johnson, col. 7:67-8:48). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the encryption step of Johnson to generate key data, wherein the circuit design data is selected to operate as targeted when the key data is inputted into the LSI after the step of converting the circuit design data into encrypted circuit design data, since the insertion of dummy data by a branch insertion transformation instills more complexity and hence better obfuscation of program design. Collberg, section 4.2, 1<sup>st</sup> paragraph. The aforementioned cover the limitations of claim 1.

15. As per claim 24, Johnson discloses a method for designing a circuit, comprising the step of encrypting provided circuit design data (Johnson, Abstract), the encrypting step includes the steps of:

- b. generating dummy circuit design data; converting the circuit design data into encrypted circuit design data by combining the circuit design data and the dummy circuit design data (Johnson, col. 12:9-20).

16. Johnson does not expressly disclose generating real key data and dummy key data, wherein the circuit design data is selected to operate as targeted with the real key data and the dummy circuit design data is selected to operate with the dummy key data, wherein the circuit design data is selected to operate as targeted when the key data is inputted into the LSI after the step of converting the circuit design data into encrypted circuit design data. Collberg discloses multiple opaque constructs wherein irrelevant code is inserted into an original code by means of a branch insertion transformation (Collberg, fig. 4(b)); a basic block is replaced with two different obfuscated versions by applying different sets of obfuscating transformations to the basic block. At runtime, a predicate selects one of two paths, the operation of the code being equivalent regardless of the selection of the paths. (Collberg, section 4.2, 3<sup>rd</sup> paragraph) This runtime value is the key data of the obfuscation technique disclosed by Collberg. This disclosure of Collberg suggests that the feature of inputting real key data and dummy key data after the step of converting the circuit design data into encrypted circuit design data are obvious implementations in the field of obfuscation of program design. Moreover, although Collberg discloses such limitations in the context of software design rather than hardware design, the two areas are closely linked: Johnson discloses that hardware design and high-level programming languages are generally encoded based on similar principles (Johnson, col. 7:67-8:48). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the encryption step of Johnson to generate a real key data and dummy key data, wherein the circuit design data is selected to operate as targeted with the real key data and the dummy circuit



design data is selected to operate with the dummy key data, wherein the circuit design data is selected to operate as targeted when the key data is inputted into the LSI after the step of converting the circuit design data into encrypted circuit design data, since conditional transformations that insert additional predicates within a program instills more complexity and hence better obfuscation of program design. Collberg, section 4.3, 1<sup>st</sup> paragraph. The aforementioned cover the limitations of claim 24.

17. As per claim 25, Johnson discloses a method for designing a circuit, comprising the step of encrypting provided circuit design data (Johnson, Abstract), the encrypting step includes the steps of:

c. generating dummy circuit design data having a same number of inputs and a same number of outputs as those of the circuit design data; converting the circuit design data into encrypted circuit design data by combining the circuit design data and the dummy circuit design data (Johnson, col. 12:9-20, especially, lines 11-14).

18. Johnson does not expressly disclose generating key data, wherein the circuit design data is selected to operate as targeted when the key data is inputted into the LSI after the step of converting the circuit design data into encrypted circuit design data. Collberg discloses multiple opaque constructs wherein irrelevant code is inserted into an original code by means of a branch insertion transformation (Collberg, fig. 4(b)); a basic block is replaced with two different obfuscated versions by applying different sets of obfuscating transformations to the basic block. At runtime, a predicate selects one of

Art Unit: 2132

two paths, the operation of the code being equivalent regardless of the selection of the paths. (Collberg, section 4.2, 3<sup>rd</sup> paragraph) This runtime value is the key data of the obfuscation technique disclosed by Collberg. Moreover, although Collberg discloses such limitations in the context of software design rather than hardware design, the two areas are closely linked: Johnson discloses that hardware design and high-level programming languages are generally encoded based on similar principles (Johnson, col. 7:67-8:48). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the encryption step of Johnson to generate key data, wherein the circuit design data is selected to operate as targeted when the key data is inputted into the LSI after the step of converting the circuit design data into encrypted circuit design data, since the insertion of dummy data by a branch insertion transformation instills more complexity and hence better obfuscation of program design. Collberg, section 4.2, 1<sup>st</sup> paragraph. The aforementioned cover the limitations of claim 25.

### ***Allowable Subject Matter***

19. Claims 2-7 are allowed.

### ***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

### ***Communications Inquiry***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should

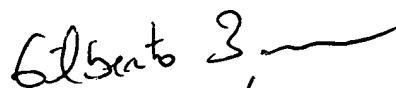
Art Unit: 2132

you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



June 9, 2006

Jung W Kim  
Examiner  
Art Unit 2132



GILBERTO BARRON JR  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100